AF

Attorney Docket # 2132-47PCON

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Harri VATANEN
Serial No.: 09/868,387
Filed: June 18, 2001
For: Method and System for Implementing a Digital Signature

Examiner: Ha, Leynna A.
Group Art: 2135

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on
July 25, 2006
(Date of Deposit)

Lance J. Lieberman
Name of applicant, assignee or Registered Representative

Signature

July 25, 2006
Date of Signature

Mail Stop **Appeal Brief - Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

07/31/2006 TBESHAH1 00000004 09868387
01 FC:1402 500.00 OP

APPEAL BRIEF

SIR:

This is an appeal, pursuant to 37 C.F.R. § 41.37 from the decision of the Examiner in the above-identified application, as set forth in the Final Office Action wherein the Examiner finally rejected appellant's claims. The rejected claims are reproduced in the Appendix A attached hereto. A Notice of Appeal was filed on May 25, 2006.

The fee of $500.00 for filing an Appeal Brief pursuant to 37 C.F.R. § 41.20 is submitted herewith. Any additional fees or charges in connection with this application may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

REAL PARTY IN INTEREST

The assignee, Sonera Smarttrust Oy, of applicant, Harri Vatanen, is the real party of interest in the above-identified U.S. Patent Application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals and/or interferences related to the above-identified application at the present time.

STATUS OF CLAIMS

Claims 1-17 have been rejected. Claims 1-17 are on appeal.

STATUS OF AMENDMENTS

There have been no Amendments filed subsequent to the Final Office Action. A response to the final Office Action was filed without amendments to the claims. The Examiner issued an Advisory Action in reply on April 12, 2006.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Independent claim 1

Independent claim 1 of Appellant's application relates to a method for digitally signing an electronic form in a secure manner by means of a mobile station. The step of "computing a first hash code for the material to be signed, the material to be signed including the form, an identifier of the form, shared information, and/or essential information" is supported at step 32 in Fig. 3; page 11, lines 1-5; and page 4, lines 11-14 of the specification. These portions of the

specification state that a hash code H1 is computed from the material, that the material to be signed includes the form, its identifier, shared data, and/or essential information added to the form.

The step of "transferring the material to be signed and the first hash code to the mobile station" is supported at step 33 in Fig. 3 and page 11, lines 5-14. The step of "digitally signing, using the mobile station, the material and first hash code transferred to the mobile station" is supported at step 37 of Fig. 3 and page 11, lines 14-20. The step of "verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature" is supported at step 40 in Fig. 3 and at page 11, lines 28-32.

Independent claim 13

Independent claim 13 is directed to a system for digitally signing an electronic form in a secure manner by a mobile station. The system comprises a payment machine 2 (page 8, line 35; and Fig. 1). The payment machine may refer to any local or locally operated automated machine capable of communication over a telecommunication network with a service provider or alternatively may be implemented locally in a computer (page 7, lines 3-10). Claim 13 further recites "means connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it" (page 8, line 36 to page 9, line 1). The generation of types of materials, i.e., bill payments and other bank or cash services, are made by terminals as described in the background section of the application. Claim 13 further recites means 4 "connected to the payment machine for the transfer of the material into the mobile station" (page 9, lines 1-5). The means 4 may be implemented using Bluetooth technology or an infrared interface (page 9, lines 5-10).

The limitation which recites "the payment machine comprises means for computing a first hash code from the material to be signed and means for transfer of the first hash code into the mobile station" is supported at page 7, lines 17-19; and page 9, lines 28-30. A hash function may be used to computing the hash code as stated at page 6, lines 16-17. The recitation "the mobile station comprises signing means for the signing of the material transferred into it" is supported at page 7, lines 19-21. The specification further describes that the signing means may comprise a memory in which the algorithms and keys required for the signature and encryption are stored, and a processor which is connected to the memory and which processes the material (page 7, lines 21-25). Support for "the payment machine comprises means for verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature" is found at page 7, lines 26-30 and page 9, lines 14-19.

GROUNDS OF REJECTION TO BE REVIEWED IN APPEAL

1. Whether claims 1-17 are patentable under 35 U.S.C. 102(e) over U.S. Patent No. 5,754,656 (Nishioka)?

ARGUMENT

INDEPENDENT CLAIM 1

Independent claim 1 recites "computing a first hash code for the material to be signed, the material to be signed including the form, an identifier of the form, shared information, and/or essential information" and "transferring the material to be signed and the first hash code to the mobile station".

MPEP §2131 states that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. V. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Nishioka fails to disclose "transferring the material to be signed and the first hash code to the mobile station" because Nishioka fails to disclose a mobile station as recited in the claims. Furthermore, Nishioka discloses that the material to be signed and the first hash code is generated by the terminal used by the user, i.e., the user site apparatus, and therefore fails to teach or suggest any need to transfer the material to another station.

Nishioka discloses an electronic shopping method. According to Nishioka, a user site apparatus 10, i.e., a terminal, is operated by a user who has a smart card 20 (see Fig. 1, and col. 9, lines 3-6 and 15-20 of Nishioka). A retail store site apparatus 30 is installed in a retail store and is connected to the user site apparatus 10 by a communication line 50 for introducing various products to the user (col. 9, lines 6-9). A credit card company site apparatus 40 is connected to the retail store site apparatus 30 by a communication line 51.

The Examiner's rejection refers to the embodiment described in cols. 21-22 of Nishioka. Accordingly, we will briefly describe that embodiment. During operation, a user inserts the smart card 20 into a slot in the user site apparatus 10 (col. 21, lines 1-3 of Nishioka). A user then selects desired products supplied from retail store site apparatus 30 and displayed on the user site apparatus 10 (col. 21, lines 5-10). The user operates an input unit such as a keyboard of the user site apparatus 10 to activate a document producing unit 102 to produce a written order P which includes a part P1 for the retail store and a part P2 for the credit card company (col. 21, lines 11-14; see also col. 10, lines 44-52). The user site apparatus 10 then produces a key K and a cipher C1 and

produces a value *u* based on a random number *r* and the key K (col. 21, lines 15-32). The value *u* is then sent from the user site apparatus 10 to the retail store site apparatus 30 (see col. 21, lines 34-37). The retail store site apparatus 30 produces a value *v* based on a random number *t* and the value *u* received from the user site apparatus 10 (col. 21, lines 38-47). The value *v* is sent back to the user site apparatus 10 (col. 21, lines 48-51).

The user site apparatus 10 calculates a hash value g(f(h(P1), P2), *v*, I), in which I is identification information and g, f, and h are hash functions, and supplies the hash value to the smart card 20 (col. 21, line 58 – col. 22, line 5). The smart card 20 then calculates a digital signature which is sent back to the user site apparatus 10 (col. 22, lines 6-11). The user site apparatus 10 then submits the signature, the value *w* and the cipher C1 to the retail store site apparatus 30.

The Examiner alleges in the Office Action and the comments on the Continuation page of the Advisory Action that the smart card 20 of Nishioka is a mobile station. The smart card 20 is installed in a slot on the user site apparatus 10 (see col. 21, lines 1-3). That is, the smart card 20 must be inserted in a slot of a terminal or other device to be used. This is evidenced by the fact that the smart card 20 as disclosed in Fig. 3 and col. 9, lines 53-61 has only a memory 202 and a enciphering/deciphering unit 201 which are both connected to the user site apparatus through a smart card input/output unit 101 on the user site apparatus 10. Accordingly, the smart card 20 itself can not be considered to be the mobile station recited in the claims. Rather, the smart card 20 is a card having memory and some functionality that is inserted into a station, such as a terminal, for working with the terminal. Since the smart card 20 of Nishioka can not be considered to be a station, Nishioka fails to disclose the limitation "transferring the material to be signed and the first hash code to the mobile station", as expressly recited in independent claim 1.

For all of the above reasons, independent claim 1 is not anticipated by Nishioka under 35 U.S.C. §102(e).

Furthermore, Nishioka discloses that the user site apparatus 10 is operated by the user with the smart card 20 inserted therein. Accordingly, the user site apparatus and not the smart card is the station utilized by a user in Nishioka. Since the user site apparatus also generates the material to be signed, there is no need to transfer the material to any other station, and especially not a mobile station, as recited in independent claim 1. Accordingly, independent claim 1 is also allowable over Nishioka under 35 U.S.C. §103.

INDEPENDENT CLAIM 13

Independent claim 13 recites "means connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it" and "means connected to the payment machine for the transfer of the material into the mobile station", and "the payment machine comprises means for computing a first hash code from the material to be signed and means for transfer of the first hash code into the mobile station".

Nishioka fails to disclose "means connected to the payment machine for the transfer of the material into the mobile station", wherein "the payment machine comprises means for computing a first hash code from the material to be signed and means for transfer of the first hash code into the mobile station", because Nishioka fails to disclose a mobile station. Furthermore, Nishioka discloses that the material to be signed and the first hash is generated by the terminal used by the user, i.e., the user site apparatus, and therefore fails to teach or suggest any need to transfer the material to another station.

In the rejection of claim 13 in the Office Action and in the comments on the Continuation page of the Advisory Action, the Examiner alleges that the smart card 20 is the mobile station and that the user site apparatus 10 and the retail store apparatus 30 are both part of the claimed payment machine. As discussed above, the smart card 20 disclosed in Nishioka can not be considered to be the mobile station because the smart card 20 must be inserted in a slot of a terminal to be used. That is, it cannot operate independently to do anything. The user site apparatus 10 is merely identified by Nishioka as a terminal and therefore fails to disclose a mobile station, as recited in independent claim 13.

Accordingly, independent claim 13 is not anticipated by Nishioka under 35 U.S.C. §102(e).

Independent claim 13 is also not obvious over Nishioka under 35 U.S.C. §103. Nishioka discloses that the user site apparatus 10 is operated by the user with the smart card 20 inserted therein. Accordingly, the user site apparatus and not the smart card is the station utilized by a user in Nishioka. Since the user site apparatus also generates the material to be signed, there is no need to transfer the material to any other station, and especially not a mobile station, as recited in independent claim 13.

In view of the above remarks, independent claims 1 and 13 are deemed to be allowable over Nishioka.

Dependent claims 2-12 and 14-17, each being dependent on one of independent claims 1 and 13, are allowable for the same reasons described above with respect to independent claims 1 and 13, as well as for the additional recitations contained therein.

For the foregoing reasons, it is respectfully submitted that the teachings of Nishioka fail to establish a *prima facie* case of anticipation with regard to the subject matter recited in claims. The Final Rejection of claims 1-17 should accordingly be reversed.

CONCLUSION

For the foregoing reasons, it is respectfully submitted that appellant's claims are not anticipated by Nishioka and are, therefore, patentable over the art of record, and the Examiner's rejections should accordingly be reversed.

Respectfully submitted,
COHEN, PONTANI, LIEBERMAN & PAVANE LLP

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: July 25, 2006

CLAIMS APPENDIX

1. (previously presented) Method for digitally signing an electronic form in a secure manner by means of a mobile station, said method comprising the steps of:

computing a first hash code for the material to be signed, the material to be signed including the form, an identifier of the form, shared information, and/or essential information;

transferring the material to be signed and the first hash code to the mobile station;

digitally signing, using the mobile station, the material and first hash code transferred to the mobile station; and

verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature.

2. (previously presented) Method as defined in claim 1, wherein the first hash code is added to the material to be transferred to the mobile station.

3. (previously presented) Method as defined in claim 1, wherein the material to be signed is generated from an identifier of the form and essential information associated with the form.

4. (previously presented) Method as defined in claim 3, wherein said step of computing comprises computing the first hash code from the material to be signed, before the material is transferred into the mobile station.

5. (previously presented) Method as defined in claim 1, wherein:

the material is transferred to the mobile station for signature from a second party; and

the signed material is transferred to the second party, whereupon the second party performs said step of verifying the authenticity of the signature.

6. (previously presented) Method as defined in claim 5, wherein:

the material is encrypted before being transferred between the mobile station and the second party; and

the encrypted material is decrypted before any treatment of the material, such as signature and verification of authenticity.

7. (previously presented) Method as defined in claim 1, wherein the form is generated using a pre-agreed form template provided with an identifier, the essential information being filled in in the form template before it is transferred to the mobile station.

8. (previously presented) Method as defined in claim 1, wherein the hash code is generated using a hash function.

9. (previously presented) Method as defined in claim 1, wherein the signature and/or encryption of the message is implemented using a public and private key method.

10. (previously presented) Method as defined in claim 1, wherein the material and/or part of it is presented in the mobile station before the material is signed.

11. (previously presented) Method as defined in claim 1, wherein the mobile station is started in signature mode before the transfer of the material into the mobile station.

12. (previously presented) Method as defined in claim 1, wherein:

the material is stamped with a time stamp; and

the transaction of signature of the material is filed after the signature has been authenticated.

13. (previously presented) System for digitally signing an electronic form in a secure manner by a mobile station (MS), said system comprising:

a payment machine;

means connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it, and

means connected to the payment machine for the transfer of the material into the mobile station, wherein

the payment machine comprises means for computing a first hash code from the material to be signed and means for transfer of the first hash code into the mobile station;

the mobile station comprises signing means for the signing of the material transferred into it; and

the payment machine comprises means for verifying the authenticity of the signed and transferred material by comparing the signed hash code with the first hash code computed from the material before signature.

14. (previously presented) System as defined in claim 13, wherein the system comprises:

a server connected to the payment machine and the mobile station and controlled by a third party; and

the mobile station comprises means for encrypting the signed material.

15. (previously presented) System as defined in claim 13, wherein the server comprises means for the verification of authenticity of the digital signature.

16. (previously presented) System as defined in claim 13, wherein the mobile station comprises means for presenting the material and/or part of the material in the mobile station before the signing of the material.

17. (previously presented) System as defined in claim 13, wherein the server comprises:

means for stamping the material with a time stamp; and

means for filing the transaction of signing of the material after the signature has been authenticated.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None